

AMENDMENTS TO THE CLAIMS

1. (Previously Presented) A data processing system for distributing and authenticating documents from a plurality of parties to a recipient data processing apparatus, the system comprising

a plurality of document distribution devices each configured to generate an original hash value from the content of an electronic file containing a document to be distributed; and

a data communications network configured to communicate each of the original hash values to the recipient data processing apparatus before a predetermined event, the recipient data processing apparatus configured to:

receive the original hash values from each of the plurality of document distribution devices via the data communication network,

generate an original super hash value from the plurality of the original hash values received, and

communicate the original super hash to the plurality of document distribution devices,

wherein after the predetermined event, the plurality of document distribution devices are configured to:

communicate each of the respective electronic files to the recipient data processing apparatus,

wherein the recipient data processing apparatus is further configured to:

generate a comparative hash value from the content of the electronic file containing the document received from each of the document distribution devices,

generate a comparative super hash value from each of the comparative hash values,

communicate the comparative super hash value to each of the document distribution devices, and

determine whether or not the documents received by the recipient data processing apparatus have changed from a comparison of at least one of the original hash values and the comparative hash values, and the comparative super hash value and the original super hash value.

2. (Previously Presented) The data processing system according to claim 1, wherein the recipient data processing apparatus is configured to identify a document which has changed by comparing each original hash value with the corresponding comparative hash value, and, if the comparative hash value is not the same as the original hash value, to determine that the corresponding document has changed.

3. (Previously Presented) The data processing system according to claim 1, wherein the original hash value generated by a document distribution device is encrypted using a private key associated with the document distribution device.

4. (Previously Presented) The data processing system according to claim 2, wherein the super hash value to be communicated to the document distribution devices is encrypted using a private key associated with the recipient data processing apparatus.

5. (Previously Presented) The data processing system according to claim 1, wherein the electronic file containing the document to be distributed is encrypted using a public key associated with the recipient data processing apparatus prior to being communicated to the recipient data processing apparatus.

6. (Previously Presented) The data processing system according to claim 1, wherein the predetermined event includes expiration of a time limit on a particular date.

7. (Previously Presented) The data processing system as claimed in claim 1, wherein the electronic file is created by an application program.

8. (Previously Presented) The data processing system as claimed in Claim 7, wherein the electronic file is communicated as part of an e-mail.

9. (Previously Presented) The data processing system as claimed in Claim 7, wherein the electronic file is communicated on a portable data storage medium to the recipient data processing device via a postal service.

10. (Previously Presented) The data processing system as claimed in Claim 9, wherein the original hash value is represented as a bar code, the bar code being arranged in association with the portable data storage medium, and wherein the recipient data processing apparatus includes a storage medium reader configured to reproduce the electronic file from the portable data storage medium, and a bar code reader for reproducing the original hash value from the bar code associated with the portable data storage medium, the electronic file representing the document being stored in association with the hash value in a data store.

11. (Previously Presented) The data processing system as claimed in Claim 7, wherein the document is generated from an on-line browser, and wherein the data communications network includes one of an intranet and the Internet.

12. (Currently Amended) A document distribution device for distributing a document to a recipient data processing apparatus via a data communications network, the document distribution device ~~comprising~~ comprising:

a data processing apparatus configured to process applications software for generating an electronic document, and to generate an original hash value from the electronic document; and

a communication interface configured to communicate the original hash value to a recipient data processing apparatus before a predetermined event via a data communications network, and, after the predetermined event, to communicate the electronic document to the recipient data processing apparatus via the data communications network.

13. (Previously Presented) The document distribution device as claimed in Claim 12, wherein the data processing apparatus is configured to receive from the recipient data processing apparatus, via the communications interface, an original super-hash value generated by the recipient data processing apparatus from a combination of the original hash value communicated by the data processing apparatus and a hash value generated by at least one other document distribution device, and to receive a comparative super hash value generated by the recipient data processing apparatus from the electronic document received from the document distribution device and at least one other electronic document received from the at least one other document distribution device.

14. (Previously Presented) The document distribution device as claimed in Claim 12, wherein the data processing apparatus is configured to encrypt the original hash value using a private key associated with the document distribution device.

15. (Currently Amended) The document distribution device as claimed in ~~Claim 14~~ Claim 13, wherein the data processing apparatus is configured to decrypt the super hash value received from recipient data processing apparatus using a private key associated with the recipient data processing apparatus.

16. (Previously Presented) The document distribution device as claimed in Claim 12, wherein the data processing apparatus is configured to encrypt the electronic file containing the document produced by the applications software using the private key associated with the document distribution device prior to being communicated to the recipient data processing apparatus.

17. (Previously Presented) The document distribution device as claimed in Claim 16, wherein the communications interface includes a recording device configured to record the electronic file on a portable data storage medium, a bar code generator operable to represent the original hash value as a bar code, and wherein the communications interface is configured to associate the bar code with the portable data storage medium.

18. (Previously Presented) The document distribution device as claimed in Claim 12, wherein the applications software provides an on-line web browser, wherein the document is generated from the on-line browser, and wherein the data communications network includes at least one of an intranet and the Internet.

19. (Previously Presented) A recipient data processing device configured to authenticate documents received from one or more document distribution devices via a data communications network, the recipient data processing device comprising:

- a communications interface configured to receive a plurality of original hash values from the document distribution devices via the data communication network before a predetermined event; and

- a data processing apparatus comprising a hashing processor configured to generate an original super hash value from the plurality of the received original hash values, and communicate the original super hash value to each of the document distribution devices, wherein the data processing apparatus is configured to operate in combination with the communications interface to

- receive, after the predetermined event, respective electronic files from the document distribution devices,

- generate a comparative hash value from the content of the electronic file containing the document received from each of the distribution devices,

- generate, using the hashing processor, a comparative super hash value from each of the comparative hash values,

communicate the comparative super hash value to the document distribution devices, and

determine whether or not the documents received by the recipient data processing apparatus have changed based a comparison of at least one of the original hash values and the comparative hash values, and the comparative super hash value and the original super hash value.

20. (Previously Presented) The recipient data processing apparatus as claimed in Claim 19, wherein the data processing apparatus is configured to identify a document which has changed by comparing each original hash value with the corresponding comparative hash value, and if the comparative hash value is not the same as the original hash value, determine that the corresponding document has changed.

21. (Previously Presented) The recipient data processing apparatus as claimed in Claim 19, wherein the original hash values received from the document distribution devices are encrypted using a private key associated with each document distribution device, and wherein the recipient data processing apparatus comprises

an encryption processor configured to decrypt the original hash values using a public key associated with the document distribution device.

22. (Previously Presented) The recipient data processing apparatus according to claim 21, wherein the encryption processor is configured to encrypt the original super hash value and the comparative super hash to be communicated to the document distribution devices in encrypted form.

23. (Previously Presented) The recipient data processing apparatus according to claim 19, wherein the encryption processor is configured to decrypt the electronic file representing the distributed document using a public key associated with the document distribution devices.

24. (Previously Presented) The recipient data processing apparatus according to Claim 19, comprising a data storage medium reader configured to reproduce the electronic file from the portable data storage medium, and a bar code reader for reproducing the original hash value from the bar code associated with the portable data storage medium, the electronic file representing the document being stored in association with the hash value in a data store.

25. (Previously Presented) The recipient data processing apparatus as claimed in claim 19, wherein the communications interface includes an on-line browser facility for generating the document, and wherein the data communications network includes one of an intranet and the Internet.

26. (Previously Presented) A computer-implemented method for distributing documents from a plurality of parties to a recipient data processing apparatus, the method comprising:

- generating, for each of the plurality of parties, an original hash value from the content of an electronic file representing a document to be distributed;

- communicating the original hash value to the recipient data processing apparatus before a predetermined event via a data communications network;

- generating, at the recipient data processing apparatus, an original super hash value from the plurality of the original hash values received;

- communicating the original super hash to the plurality of document distribution devices; and, after the predetermined event,

- communicating, from the plurality of document distribution devices, each of the respective electronic files to the recipient data processing apparatus;

- generating, at the recipient data processing apparatus, a comparative hash value from the content of the electronic file containing the document received from each of the distribution devices;

- generating a comparative super hash value from each of the comparative hash values; and

- determining whether or not the documents received by the recipient data processing apparatus have changed based on a comparison of at least one of the original hash values and the comparative hash values, and the comparative super hash value and the original super hash value.

27. (Previously Presented) The data processing method according to Claim 26, further comprising:

- identifying a document which has changed by comparing each original hash value with the corresponding comparative hash value, and if the comparative hash value is not the same as the original hash value,

determining that the corresponding document has changed.

28. (Currently Amended) A method for distributing documents to a recipient data processing device via a data communications network, the method ~~comprising~~ comprising:

generating an electronic document;

generating an original hash value from the electronic document; and

communicating the original hash value to a recipient data processing apparatus before a predetermined event via a data communications network, and, after the predetermined event, communicating the electronic document to the recipient data processing apparatus via the data communications network.

29. (Previously Presented) The method as claimed in Claim 27, further comprising:

receiving, from the recipient data processing apparatus, an original super-hash value generated by the recipient data processing apparatus from a combination of the original hash value communicated by the data processing apparatus and a hash value generated by at least one other document distribution device; and

receiving a comparative super hash value generated by the recipient data processing apparatus from the electronic document received from the document distribution apparatus and at least one other electronic document received from the at least one other document distribution device.

30. (Previously Presented) A method of authenticating documents received from a plurality of document distribution devices via a data communications network, the method comprising:

receiving a plurality of original hash values from the document distribution devices, before a predetermined event, via the data communication network;

generating an original super hash value from the plurality of the original hash values received;

communicating the original super hash value to each of the document distribution devices;

receiving, after the predetermined event, respective electronic files from document distribution devices;

generating a comparative hash value from the content of the electronic file containing the document received from each of the distribution devices;

generating a comparative super hash value from each of the comparative hash values;

communicating the comparative super hash value to the document distribution devices; and

determining whether or not the documents received by the recipient data processing apparatus have changed based on a comparison of at least one of the original hash values, and the comparative hash value and the comparative super hash value and the original super hash value.

31. (Currently Amended) A non-transitory computer readable medium having a program for executing a method of distributing documents to a recipient data processing device via a data communications network, the method ~~comprising~~ comprising:

generating an electronic document;

generating an original hash value from the electronic document; and

communicating the original hash value to a recipient data processing apparatus before a predetermined event via a data communications network, and, after the predetermined event, communicating the electronic document to the recipient data processing apparatus via the data communications network.

32. (Previously Presented) A non-transitory computer readable medium having a program for executing a method of authenticating documents received from a plurality of document distribution devices via a data communications network, the method comprising:

receiving a plurality of original hash values from the document distribution devices, before a predetermined event, via the data communication network;

generating an original super hash value from the plurality of the original hash values received;

communicating the original super hash value to each of the document distribution devices;

receiving, after the predetermined event, respective electronic files from document distribution devices;

generating a comparative hash value from the content of the electronic file containing the document received from each of the distribution devices;

generating a comparative super hash value from each of the comparative hash values;

communicating the comparative super hash value to the document distribution devices; and

determining whether or not the documents received by the recipient data processing apparatus have changed based on a comparison of at least one of the original hash values, and the comparative hash value and the comparative super hash value and the original super hash value..

33. (Canceled)

34. (Currently Amended) A data processing apparatus for ~~distributing~~ distributing documents from a plurality of parties to a recipient data processing apparatus, the apparatus comprising:

means for generating, for each of the plurality of parties, an original hash value from the content of an electronic file representing a document to be distributed;

means for communicating the original hash value to the recipient data processing apparatus, before a predetermined event, via a data communications network;

means for generating, at the recipient data processing apparatus, an original super hash value from the plurality of the original hash values received;

means for communicating the original super hash to the plurality of document distribution devices;

means for communicating, after the predetermined event, from the plurality of document distribution devices, each of the respective electronic files to the recipient data processing apparatus;

means for generating, after the predetermined event, at the recipient data processing apparatus, a comparative hash value from the content of the electronic file containing the document received from each of the distribution devices;

means for generating, after the predetermined event, a comparative super hash value from each of the comparative hash values; and

means for determining whether or not the documents received by the recipient data processing apparatus have changed based on a comparison of at least one of the original hash values and the comparative hash values, and the comparative super hash value and the original super hash value.

35. (Canceled)

36. (Canceled)